REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-03-2008	FINAL	

4. TITLE AND SUBTITLE

What Happens when the Lights Go Out:

Airpower Vulnerabilities in the Era of Network Centric Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LT Matthew D. Culp

Paper Advisor (if Any): CAPT James K. Cook

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

14. ABSTRACT

Technological superiority has played an important role in the dominance of U.S. airpower, but the organization of the command and control structure has also been crucial. For years, the "master tenet" of airpower has been centralized control with decentralized execution. But a combination of factors including technology, collateral damage concerns, and dynamic targeting requirements have caused execution authority to become increasingly centralized in recent operations. This trend has resulted in a growing tendency for operational commanders, such as the Join Force Air Combatant Commander (JFACC), to direct action at the tactical level.

In the era of Network-Centric Warfare, command and control (C^2) organizations increasingly depend on complex communications systems and networks. DOD infrastructure has not kept pace with rapidly growing bandwidth requirements, leading to a heavy reliance on more vulnerable commercial systems. As a result, C^2 organizations are becoming more vulnerable to physical, electronic, and cyber attacks, and the complexity of communications networks makes it impossible to predict the consequences of a multi-faceted attack.

The critical importance of reliable communications requires that these issues be addressed. But more important, forces and C^2 organizations must train to the vulnerabilities and limitations of technology. Mission based orders, adherence to the master tenet, and delegation of execution authority remain crucial in preserving the war-fighter's initiative and providing airpower the flexibility to

15. SUBJECT TERMS

Joint Force Air Component Commander, JFACC, Command and Control, C2, Network-Centric Warfare, Time Sensitive Targeting, Centralized Control, Air Operations Center, Airpower, Bandwidth, Communication Systems, Commercial Satellites

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		27	19b. TELEPHONE NUMBER *(include area code)* 401-841-4120

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

What Happens when the Lights Go Out:

Airpower Vulnerabilities in the Era of Network Centric Warfare

By

Matthew D. Culp

LT, USN

A paper submitted to the Provost, Naval War College, for consideration in the Prize Essay Competition in the Military Officers Association of America (MOAA) category.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____

27 May 2008

Contents

Abstract

Technological superiority has played an important role in the dominance of U.S. airpower, but the organization of the command and control structure has also been crucial. For years, the "master tenet" of airpower has been centralized control with decentralized execution. But a combination of factors including technology, collateral damage concerns, and dynamic targeting requirements have caused execution authority to become increasingly centralized in recent operations. This trend has resulted in a growing tendency for operational commanders, such as the Join Force Air Combatant Commander (JFACC), to direct action at the tactical level.

In the era of Network-Centric Warfare, command and control (C^2) organizations increasingly depend on complex communications systems and networks. DOD infrastructure has not kept pace with rapidly growing bandwidth requirements, leading to a heavy reliance on more vulnerable commercial systems. As a result, C^2 organizations are becoming more vulnerable to physical, electronic, and cyber attacks, and the complexity of communications networks makes it impossible to predict the consequences of a multi-faceted attack.

The critical importance of reliable communications requires that these issues be addressed. But more important, forces and C^2 organizations must train to the vulnerabilities and limitations of technology. Mission based orders, adherence to the master tenet, and delegation of execution authority remain crucial in preserving the war-fighter's initiative and providing airpower the flexibility to dominate the skies in combat operations of the future.

INTRODUCTION

Over the years, centralized command and control has been a major factor in allowing U.S. forces to maintain air supremacy and to provide responsive on-call airpower in support of ground forces. From Operations DESERT STORM to IRAQI FREEDOM, American and coalition airpower has been dominant. Technological superiority has played an important role. But the organization of the command and control structure has been crucial in giving airpower the flexibility to adapt to changing conditions on the battlefield.

Atop airpower's command and control structure is the Joint Force Air Component Commander (JFACC). The JFACC has operational control of air assets in theater and exerts this control through the promulgation of the air tasking order. This order is both written and executed by the JFACC's subordinate command and control agency, the air operations center (AOC). Functionally, the AOC is a highly complex organization containing a large number of personnel supported by an array of communications systems and computer networks that manage the enormous amount of information required to conduct modern air-combat operations.

Although for many years the "master tenet" of airpower has been centralized control with decentralized execution, recent operations have increasingly been centrally executed. Improvements in communications systems and network technologies have given operational commanders, such as the JFACC, unprecedented availability of highly detailed information. As a consequence, there is a growing tendency to use this information to direct action at the tactical level.

This paper will demonstrate that the trend toward centralized execution of airpower, combined with a growing dependence on complex networks and rapidly increasing needs for bandwidth, has potentially disastrous consequences. Despite recent operational successes, the JFACC's command and control structure is steadily becoming a critical vulnerability for U.S. airpower and, by extension, future military operations as a whole.

The following pages will examine the evolution of the "master tenet" and the trend toward increasingly centralized execution. Resulting vulnerabilities of the AOC's ability to function in a hostile environment will be discussed. In addition, the implications of successful exploitation of these vulnerabilities by an enemy will be examined. Finally, recommendations will be made to mitigate the risk and minimize the potential consequences of an attack.

DEFINITIONS

Joint Publication (JP) 1-02 defines centralized control as "placing within one commander the responsibility and authority for planning, directing, and coordinating a [joint] military operation or group/category of operations."[i] Decentralized execution is defined as "delegation of execution authority to subordinate commanders."[ii]

For centralized execution, this paper will use the definition proposed by Lt Col Woody Parramore: "Centralized execution happens if a sortie carries out its mission under direct control of an air operations center… with no other echelon in the chain of command issuing orders."[iii] This definition will include situations where a subordinate

element of the theater air control system (e.g., an airborne controller), relays a targeting order or a weapons release authorization from the AOC to a tactical platform.

THE EVOLUTION OF THE MASTER TENET AND THE MODERN AOC

> *"Airpower is indivisible. If you split it up into compartments, you merely pull it to pieces and destroy its greatest asset – its flexibility."*[iv]
>
> – Field Marshall Sir Bernard Montgomery

World Wars I and II

The concept of centralized control of airpower has its origins as far back as World War I, when Brig. General William "Billy" Mitchell coordinated employment of 1,500 aircraft in support of the 1918 St. Mihiel Offensive[v].

During World War II, at Kasserine Pass in North Africa, the Allies held numerical superiority over Axis aircraft, but a dispersed command and control organization could not focus their efforts and capitalize on their advantage. The importance of massing airpower in a coordinated effort against specific objectives was a lesson that lasted for the duration of the war. Subsequent operations, such as those in the Southwest Pacific Area and the strategic bombing campaign of the European Theater, were unified under the control of a single commander.[vi] In 1943 this practice was written into doctrine with the publication of Field Manual 100-20 which stated, "Control of available airpower must be centralized."[vii]

The Vietnam War

Despite the lessons of World War I and II, U.S. forces failed to centralize control over air operations in Vietnam. Operations "amounted to a patchwork of service-centric operations" where rules of engagement required that target selection be "vetted at the highest levels of government."[viii]

Despite this failure, valuable lessons were learned from the distinct command and control (C^2) methods that evolved within two separate organizations. In South Vietnam, airpower was controlled by the 7th Air Force Tactical Air Control Center (TACC) and focused primarily on supporting ground forces. A sustained requirement for responsive close air support (CAS) forged an efficient C^2 structure and a network of forward air controllers (FACs) that provided rapid target identification and control of strike aircraft. [ix]

In North Vietnam, airpower was predominantly controlled by the 7th Air Force Command Center (7 AFCC)[x] which functioned quite differently from the TACC in the South. Without a similarly heavy requirement to provide CAS, there was less impetus to develop a highly responsive system; the focus was primarily on bombing strategic targets that had been picked by higher authority and could be planned well in advance.[xi]

The Vietnam War solidified the Air Force's institutional belief that airpower must be centrally controlled not by a politician, but by a single Airman and decentrally executed. In 1971 this was doctrinally published in Air Force Manual (AFM) 1-1.[xii] Today, this "master tenet" of airpower is found in Air Force Doctrine Document (AFDD) -1: "Centralized control and decentralized execution… are critical to effective employment of air and space power. Indeed, they are the fundamental organizing

principles… having been proven over decades of experience as the most effective and efficient means of employing air and space power."[xiii]

The Cold War

In the years following Vietnam, the focus on the defense of NATO from Soviet forces led to the development of the AirLand Battle Plan. Developed jointly by the Army and the Air Force, planning was divided into Close, Integrated, and Deep; for battles within 24-hours, battles 24 to 48-hours out, and those greater than 72-hours out, respectively. This 72-hour planning cycle formed the original model for the air tasking order (ATO) of today.[xiv]

The Gulf War

The JFACC concept was born as the military services struggled to adopt "jointness" following the Goldwater-Nichols Act of 1986.[xv] Five years later, Operation DESERT STORM provided the first combat test of the JFACC's ability to command and integrate joint air operations on a large scale.[xvi]

The JFACC had numerous responsibilities, including acting as the airspace control authority (ACA), providing deconfliction of air assets, and translating the Master Attack Plan (MAP) into a flyable ATO.[xvii] The air campaign showcased impressive advances in technology and precision weaponry, but its success was largely due to the organizational structure of the JFACC and served as validation of the master tenet.[xviii]

Despite the campaign's successes, significant issues of joint interoperability remained. For example, incompatible Air Force and Navy electronic communication systems resulted in the requirement for printed copies of the ATO to be flown out to

aircraft carriers in the Gulf.[xix] But in the new "joint era," the lessons of DESERT STORM provided the military services enormous incentive to improve communications compatibility.

Beyond the lessons in jointness, however, was the growing awareness of the limitations of the ATO's 72-hour planning cycle. Strikes against mobile targets, or against targets that had emerged inside the planning cycle, proved to be a difficult challenge. When the ground campaign began, fully 40% of strike sorties were being modified prior to execution. More significantly, despite the high number of assets that were tasked to the mission, very few of the dynamic, high-value targets, such as SCUD missiles, were ever destroyed.[xx]

THE TREND TOWARD CENTRALIZED EXECUTION

Little progress was made on improving the dynamic targeting process following DESERT STORM and the issue resurfaced in 1999 during Operation ALLIED FORCE. As the focus of the effort shifted from strategic bombardment to the destruction of Serbian Army and Militia forces, a significant portion of targets began to emerge inside the ATO cycle timeline. To address this, the Flex Targeting Cell was created within the AOC. "Flex targeting" was conducted through the use of airborne alert aircraft, or the reassignment of assets tasked to hit pre-planned targets on the ATO.[xxi,xxii]

The ad-hoc nature of the Flex Targeting Cell, along with emphasis on avoiding collateral damage, resulted in highly centralized execution of these dynamic missions. Target approval and engagement authority was rarely delegated and strictly resided

within the AOC, often with the JFACC himself, the Combined Forces Commander (CFC), or senior political leadership.[xxiii]

At times, centralized execution resulted in increased risk for tactical aircraft, a substantial loss of tactical flexibility, and missed opportunities to destroy potentially important targets. In one instance, an A-10 had to wait for more than 30 minutes while the AOC debated how best to attack a cache of surface-to-air missiles located near a group of houses. Finally approving the strike, the AOC provided the pilot guidance to "not hit any houses." In the meantime, clouds had obscured the target and the opportunity was lost.[xxiv]

Also of significance was the growing use of unmanned aerial vehicles (UAVs), such as Predator. For the first time, operation level commanders could receive real-time video from the tactical level, which could offer enormous temptation to reach forward and micromanage tactical action. An example of this was recounted by Lt Gen Michael Short, Commander, Allied Air Forces Southern Europe (COMAIRSOUTH):

> Real-time targeting. I will share a story. About 45 days into the war, Predator was providing great coverage for us. About 5 o'clock in the afternoon we had live Predator video of three tanks moving down the road in Serbia and Kosovo. As most of you know, my son is an A-10 pilot or he was at the time. We had a FAC overhead and General Clark [SACEUR] had the same live Predator video that I had. "Mike, I want you to kill those tanks." We had a Weapons School graduate on the phone talking directly to the FAC on the radio. Two or three minutes went by, and [the FAC] clearly had not found those tanks. The young major's [Weapons School graduate] voice went up a bit and said, "COMAIRSOUTH and SACEUR are real interested in killing those tanks. Have you got them yet?" "Negative." About two more minutes went by and the Weapons School graduate played his last card. "General Short really wants those tanks killed." And a voice came back that I've heard in my house for the better part of 30 years and he said, "[expletive deleted] it, Dad, I can't see the [expletive deleted] tanks!"[xxv]

Although humorous, the story exemplifies how such detailed awareness can easily tempt an operational level commander to focus on individual tactical action and potentially lose sight of the larger operational picture.

Using the lessons learned from ALLIED FORCE, the dynamic targeting process was clarified in the 2001 publication of JP 3-60, *Joint Doctrine for Targeting.* For the operations that followed, dynamic targeting would be carried out by the Time Sensitive Targeting (TST) cell within the AOC. In Afghanistan, as in Kosovo, the mitigation of collateral damage was a serious concern. Final approval for most TST missions was centralized at the senior levels of U.S. Central Command (CENTCOM) or Air Forces Central (CENTAF), with leadership targets requiring approval from the Secretary of Defense. Also similar to Kosovo was the effort's focus on the destruction of dispersed enemy forces, and not on fixed, pre-planned targets. For Carrier Air Wing 8, more than 80% of strike missions were launched without an assigned target. Except for those aircraft handed off to provide CAS, the balance of these were centrally executed TST sorties. [xxvi]

By the beginning of Operation IRAQI FREEDOM in March 2003, many significant improvements in the TST process had been implemented. Along with the publication of the *Commander's Handbook for Joint Time Sensitive Targeting* by the Joint Forces Command, a combined effort of Air Force and Navy exercises had resulted in the development of TST-specific Tactics, Techniques, and Procedures (TTPs). Perhaps most importantly, detailed collateral damage estimate (CDE) and positive identification criteria were established, allowing execution authority to be delegated to

subordinate commanders. Despite these advances, however, delegation was still not extended beyond the confines of the AOC.[xxvii]

VULNERABILITIES OF THE AOC

Physical Vulnerabilities

The majority of the JFACC's critical functions, such as planning, coordination, creation of the ATO, and controlling airborne forces, are executed by the air operations center. Most of these functions have no reliable backup. The central location of so many crucial C^2 functions creates a significant risk; a successful attack on the AOC would be catastrophic to combat operations.[xxviii]

In terms of preventing a physical attack, the AOC's sheer size presents a considerable challenge. The number of personnel involved, which varies in relation to the scale of an operation, is significant. For Operations ENDURING FREEDOM and IRAQI FREEDOM, the air operations center was manned, respectively, by 720 and 1966 personnel (roughly 1.4 persons per average daily sortie). By contrast, a much larger AOC organization was used to control multinational air operations for ALLIED FORCE; in Kosovo the AOC consisted of almost 2500 personnel (almost 3.1 persons per average daily sortie).[xxix]

Although an in-depth discussion of the physical vulnerabilities of the AOC is beyond the scope of this paper, it should be recognized that preventing a physical attack on the AOC is crucial to the success of U.S. operations. The capability of an enemy to strike the AOC must be carefully considered when selecting its location.

The maturation of Network Centric Warfare (NCW) provides significant potential to decrease the physical risk. Dispersing the physical locations of the AOC's functions and creating a "virtual AOC" significantly reduces the possibility of a physical attack delivering a crippling blow to the JFACC's ability to run the war. In addition, NCW gives the added benefit of "reachback," a term that refers to the utilization of the expertise of established facilities far removed from the battlefield. Reachback has the potential to greatly reduce the inevitable friction internal to a new command and ease the significant logistical challenge of forward deploying a full complement of AOC personnel and equipment.[xxx]

However, there is a trade-off to reducing the physical risk by creating a virtual AOC. By physically separating the various cells of the AOC, the organization becomes functionally dependent on the network that connects these cells together and, by extension, on the communications infrastructure that the network requires.

Network Vulnerabilities

The first and foremost requirement for the AOC to function in a network-centric environment is adequate bandwidth. As U.S. forces become increasingly networked by data-link systems, bandwidth requirements increase. UAVs such as Predator and Global Hawk further complicate the problem – in Operation ENDURING FREEDOM, Global Hawk alone consumed five-times the entire bandwidth used in DESERT STORM.[xxxi] And *peak* bandwidth usage was 30-times greater in IRAQI FREEDOM than in DESERT STORM.[xxxii]

Military communications satellites only can provide a small portion of this enormous requirement. Furthermore, the shortfall is expanding as growing bandwidth

requirements are significantly outpacing increases in capacity. This shortfall has led to a rapidly growing reliance on commercial systems. According to Lt Gen Harry Raduege of the Defense Information Systems Agency (DISA), "in Operation ENDURING FREEDOM, we're supporting one-tenth the number of forces deployed during DESERT STORM with eight times the commercial [satellite communications] bandwidth."[xxxiii] In 2005, commercial systems were handling more than 75% of operational communications requirements.[xxxiv]

It must be emphasized that the above statistics describe the bandwidth requirements of a traditional, centralized AOC. With the creation of a *virtual* AOC, bandwidth requirements will increase dramatically. Physically separate cells will require that the enormous internal AOC dataflow be moved from a local network to a global network that is increasingly reliant on commercial systems.

Communications Vulnerabilities

Satellite communications can be physically disrupted by attacks on the satellite itself, on communications nodes, or on ground stations that communicate with the satellite. In 2007, the Chinese successfully tested a new Anti-Satellite (ASAT) system by shooting down a satellite more than 500 miles in space.[xxxv] The Chinese have also been developing ASAT directed-energy weapons and improving their ability to track and identify satellites in orbit, a critical ASAT capability.[xxxvi]

Along with the threat of physical attack is the use of electromagnetic energy to disrupt signals, or jamming. Jamming poses a significant threat to satellite communications, particularly on unprotected commercial systems. Most communications satellites are in geosynchronous earth orbit so that antennas do not need to be constantly

re-aimed. Unfortunately, this makes employing a jammer against them relatively easy, and their wide coverage means that they can also be jammed from relatively large distances. Ground-based uplink jammers are relatively unsophisticated, easy to acquire and simple to employ. Jammers with proven effectiveness against commercial satellites are available through commercial suppliers for as little as $30,000 and nuisance jammers can be constructed using readily available components for under $1000. [xxxvii]

In addition to jamming, there is a problem of access. Without adequate organic resources to handle communications, the military is becoming increasingly dependent on commercially leased systems to conduct combat operations. In today's global economy, the possibility of a corporation deciding to preserve its neutrality in a conflict and refusing to lease its satellites for military use cannot be discounted.

Security implications are perhaps the most serious issue. In addition to greater susceptibility to jamming, communications over commercial networks are more easily intercepted. According to the Advanced Military Satellite Communications Capstone Requirements Document, "Current commercial systems lack sufficient protection required to support many military requirements against deliberate disruption and exploitation."[xxxviii]

Software Vulnerabilities

In an effort to increase compatibility, the software utilized across military networks is becoming increasing integrated. However, following a GAO recommendation, it is a common practice for DOD contractors to outsource software development to smaller firms as a cost-cutting measure. "In some cases, programming work may be done by offshore companies."[xxxix]

Outsourcing the programming of vital communications software is problematic in several ways. Most significantly, open-source and proprietary software often contain "back-doors" left by programmers that allow easy access to the software's coding. Although generally intended to enable better software support, these back-doors could allow the compromise of sensitive communications, or even be used to shut down an entire system. "It is virtually impossible to find unauthorized and malevolent code hidden deep within a sophisticated computer program."[xl]

Cyber Attacks

In addition to developing robust ASAT and jamming equipment, the Chinese People's Liberation Army (PLA) has been aggressively developing cyber warfare capabilities. Included in the efforts are both network attack and espionage programs. "The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to incorporate offensive CNO [computer network operations] into its exercises, primarily in first strikes against enemy networks."[xli]

Numerous attacks on DOD systems have been reported, and many have been successful. In 2003, a series of incursions into DOD systems by the Chinese were serious enough that the cyber campaign was given a codename: Titan Rain.[xlii] In June 2007, the *Financial Times* reported that a computer system in the office of Secretary of Defense Robert Gates was shut down for over a week after being hacked, presumably by the PLA. "The PLA has demonstrated the ability to conduct attacks that disable our system...and

the ability in a conflict situation to re-enter and disrupt on a very large scale," said a former official.[xliii]

Even if an adversary lacks a robust military cyber-warfare program, the threat of computer attacks cannot be ignored. As a recent RAND study notes, "computer hacker skills are essentially universal"[xliv] and that there is widespread capability such that "virtually any potential enemy… could mount some kind of information attack."[xlv]

CONCLUSIONS

For the Joint Force Air Component Commander, the line between operational and tactical control has become increasingly blurred. In recent operations, a combination of factors including technology, collateral damage concerns, and the need for better dynamic targeting have produced a steady increase in the level of centralized execution of airpower. This shift away from the master tenet has frequently resulted in operational level commanders simultaneously wielding both operational and tactical level control.

Furthermore, when execution authority remains centralized in a single command and control organization, a significant vulnerability is created. As the transition toward network-centric warfare continues, the effective function of C^2 organizations like the air operations center will become increasingly reliant on potentially vulnerable global networks and communications systems.

The great "unknown" of cyber-warfare is how far-reaching the effects of an attack could be. For instance, in 1998 the unexpected failure of a single commercial satellite led to the loss of pager service for tens of millions of Americans and the disruption of television and radio.[xlvi] In early 2000, a computer system unexpectedly failed and shut

down the National Security Agency (NSA) Headquarters; U.S. intelligence was left "virtually deaf" for 3 days.[xlvii]

The complexity of the systems relied upon by the AOC makes it similarly impossible to predict the consequences of a determined, multi-faceted attack. The effects of such an attack could be minor. For example, a jammed satellite could cause a temporary bandwidth reduction until communications are re-routed. Alternatively, the effects could be as extreme as a complete failure of the communications network at a critical moment in combat. The duration of these effects are similarly unpredictable, from minutes to days or weeks, depending on the severity and scope of the damage.

These vulnerabilities do not invalidate the concepts of Network-Centric Warfare, nor do they call into question the value or wisdom of centrally controlling airpower under the JFACC. However, these vulnerabilities, in combination with a trend toward increasingly centralized execution, have created a critical vulnerability for U.S. airpower. These vulnerabilities must be adequately addressed.

RECOMMENDATIONS

The increasing demand for bandwidth is a reality that must be faced. For NCW to be successful, vulnerabilities in communications systems must be addressed. In the short term, military dependence on commercial satellite systems is unavoidable, but the accompanying risks must be minimized. The DOD must do more than simply award communications contracts to the lowest bidder. Before relying on these vital communication systems in combat, a baseline requirement to resist jamming and exploitation must be established. Additionally, there needs to be oversight and

verification that communications are not being intercepted or exploited. Aggressive efforts are necessary to ensure that the most sensitive military communications remain confined to DOD networks.

The vulnerabilities of commercial systems to jamming and exploitation potentially limit their viability for military use, particularly in a conflict against an advanced adversary. Furthermore, unrestricted access to commercial satellites cannot be assured. In the event that commercial systems are made unavailable, bandwidth for critical communications will have to be supplied by other means. It is crucial for military communication systems to maintain a minimally adequate capability to support combat operations.

The threat of cyber attacks must be taken seriously. To cut costs, some of the military's most secure networks, such as the Secret Internet Protocol Router Network (SIPRNET), have been connected to the Non-Classified NIPRNET, in which roughly 70 percent of the traffic is routed through the civilian internet.[xlviii,xlix] Potentially exposing extremely sensitive data to attacks on the civilian internet is a risk that must not be taken lightly, regardless of the cost savings it delivers.

At a human level, centralized control with decentralized execution is, and should remain, the master tenet of airpower. But there is no reason to deny an operational commander the *ability* to centrally execute when the situation demands. The two concepts are not mutually exclusive. The effective functioning of the Time Sensitive Targeting (TST) cell in OIF is an example of the value of centralized execution in the broader context of an ongoing, largely decentralized operation. Furthermore, efforts

directed at streamlining the ATO process, shortening the "kill chain" and increasing the responsiveness of airpower must continue.

The challenge is to ensure that centralized execution remains the exception, not the rule. Even at the level of a functional component commander, the majority of a career has been spent thinking and leading at the tactical level. Unless robust air operations are in progress, it is even possible that the JFACC could have the situational awareness to direct operations down at the tactical level, while still maintaining an operational level perspective. However, this is not his job. The temptation to step in and influence tactical execution should be resisted unless the situation absolutely requires intervention. Mitigating this temptation is perhaps beyond the scope of doctrine, and might be more appropriately addressed as a key tenet of leadership.

In the modern era of the 24-hour news cycle, tactical actions and decisions often can result in strategic level consequences. Potential backlash from civilian casualties coupled with an ability to watch streaming video from the battlefield might provide the JFACC ample enticement to restrict weapons release authority to his immediate or near-immediate control. But C^2 networks and communication systems will never be 100% dependable and rules of engagement need to be written accordingly. When ground forces require close air support, or high-value, dynamic targets are found, aviators, FACs, and airborne controllers should have guidance and authority to make autonomous collateral damage estimates. Platforms such as AWACS and HAWKEYE must be free to act as more than communications relays between tactical aircraft and the AOC. They should have authority to make targeting decisions in the event of a loss of communications with the AOC.

Finally, there is a crucial requirement in training. As the technology that enables network-centric warfare becomes commonplace, the greatest challenge will be for military forces, from the combatant commander to the private on the ground, to actively avoid becoming reliant on the technology. Tactical training should routinely be conducted without the benefit of the data-link systems. At an operational level, not only should contingency plans be written for network failures, but exercises should be conducted with unpredictable and varied system degradations. False data should be injected into the network to simulate an undetected cyber attack, and the potential consequences investigated. While "Red" teams stress the system to find its vulnerabilities, "Blue" teams must find workable solutions to network outages and communications failures. Progress can be made in the planning process, but it is essential to recognize that the best solutions will be found under pressure.

– – –

Network-Centric Warfare has great potential to provide unprecedented levels of situational awareness to operational commanders and tactical forces alike. New technologies hold promise to improve coordination, accelerate responsiveness, reduce the fog of war and give combat forces lethal effectiveness. But warfare remains a human enterprise. Failing to train to the limitations and vulnerabilities of technology could easily prove to be a lethal mistake.

Ultimately, for operational commanders such as the JFACC, the importance of mission based orders, trust in one's operators, and the fervent belief in the importance of the war-fighter's initiative remain paramount.

NOTES

[i] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* as Amended through 4 March 2008, Joint Publication (JP) 1-02 (Washington, DC: 12 April 2001), 81. http://www.dtic.mil (accessed 22 April 2008).

[ii] Ibid., 145.

[iii] Woody W Parramore, "Defining Decentralized Execution in Order to Recognize Centralized Execution," *Air & Space Power Journal*, 1 October 2004, 25. http://www.proquest.com/ (accessed 22 April, 2008).

[iv] Marcus Hurley, "JFACC – Taking the Next Step," *Joint Forces Quarterly* No. 7 (Spring 1995):62. http://www.dtic.mil/ (accessed 22 April 2008).

[v] Maxwell J. Shuman, "Bringing a Grenade to a Knife Fight: Historical and Current Trends Challenge the Future Viability of the JFACC," (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007), 3. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA476778

[vi] John J. Schaefer III, "Time for a New Master Tenet?" (research paper, Ft. Leavenworth, KS: School of Advanced Military Studies, 2006), 6. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA450629

[vii] War Department, *Command and Employment of Airpower*, War Department Field Manual (FM) 100-20 (Washington, DC: GPO, 21 July 1943), I-3. http://www.au.af.mil/ (accessed 22 April 2008).

[viii] Shuman, "Bringing a Grenade," 5.

[ix] J.T. Sink, "Rethinking the Air Operations Center: Air Force Command and Control in Conventional War," (research paper, Maxwell AFB, AL: School of Advanced Airpower Studies, 1994), 19. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA285444

[x] Ibid., 18.

[xi] Ibid., 22.

[xii] Mustafa R. Koprucu, "The Limits of Decentralized Execution: The Effects of Technology on a Central Airpower Tenet," (research paper, Maxwell AFB, AL: School

of Advanced Airpower Studies, 2001), 1. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA407879

[xiii] U.S. Air Force, *Air Force Basic Doctrine,* Air Force Doctrine Document (AFDD) 1 (Washington, DC: Department of the Air Force, 17 November 2003), ix. http://www.dtic.mil/ (accessed 22 April 2008).

[xiv] Shuman, "Bringing a Grenade," 5.

[xv] Lynne M. Champagne, "Let's Put 'Joint' Back into JFACC," (research paper, Newport, RI: U.S. Naval War College, Department of Military Operations, 1994), 9. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA283537

[xvi] Hurley, "Taking the Next Step," 60.

[xvii] Deputy Chief of Staff, Plans and Operations Headquarters, United States Air Force, *JFACC Primer* (Washington, DC: Headquarters Department of the Air Force, 10 January 1994), 6. http://www.fas.org/ (accessed 22 April 2008).

[xviii] Eliot A. Cohen, "The Mystique of U.S. Air Power," *Foreign Affairs* 73, no. 1 (1 January 1994): 116. http://www.proquest.com/ (accessed 22 April, 2008).

[xix] Champagne, "Put the Joint Back in JFACC," 2.

[xx] Shuman, "Bringing a Grenade," 9.

[xxi] Robert P. Winkler, "The Evolution of the Joint ATO Cycle," (research paper, Norfolk, VA: Joint Forces Staff College, 2006), 22. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA451239

[xxii] John M. Fyfe, "The Evolution of Time Sensitive Targeting: Operation Iraqi Freedom Results and Lessons," (research paper no. 2005-02, Maxwell AFB, AL: Airpower Research Institute, 2005), 6-7. http://stinet.dtic.mil/ (accessed 22 April 2008). Available as Defense Technical Information Center (DTIC) Report ADA476994

[xxiii] Ibid., 7.

[xxiv]Schaeffer, "Centralized Execution in the Air Force," 16.

[xxv] Koprucu, "Limits of Decentralized Execution," 71.

[xxvi] Fyfe, "The Evolution of TST," 11.

[xxvii] Ibid., 15.

[xxviii] William A. Woodcock, "The Joint Forces Air Command Problem: Is Network-Centric Warfare the Answer?" *Naval War College Review* 56, no. 1 (1 January 2003): 126. http://www.proquest.com/ (accessed 22 April 2008).

[xxix]David A. Brumbaugh, "The Parallel Air Tasking Order: Reducing the Size of the Air Operations Center," (paper presented to the 2004 Command and Control Research and Technology Symposium, Chantilly, VA: Science Applications International Corp. (SAIC)), 11. http://www.dodccrp.org/ (accessed 22 April 2008).

[xxx] Woodcock, "Is NCW the Answer?" 128.

[xxxi] Kurt A. Klausner, "Command and Control of Air and Space Forces Requires Significant Attention to Bandwidth," *Aerospace Power Journal*, 1 January 2002, 72. http://www.proquest.com/ (accessed 22 April 2008).

[xxxii] Clay Wilson, "Network Centric Operations: Background and Oversight Issues for Congress," CRS Report RL32411 (Washington, DC: Congressional Research Service, 15 March 2007), 25. http://www.fas.org/ (accessed 22 April 2008).

[xxxiii]Klausner, "Attention to Bandwidth," 72.

[xxxiv] Adam J. Hebert, "Toward Supremacy in Space," *Air Force Magazine*, 1 January 2005, 27. http://www.afa.org/ (accessed 22 April 2008).

[xxxv] Simon Elegant and Mark Thompson, "Why China's Missile Test Is Troubling," *TIME*, 19 January 2007. http://www.time.com/ (accessed 22 April 2008).

[xxxvi] U.S. Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China – 2008* (Washington, DC: Office of the Secretary of Defense, 2008), 28. http:// hongkong.usconsulate.gov/ (accessed 22 April 2008).

[xxxvii] Timothy Bonds et al., *Employing Commercial Satellite Communications: Wideband Investment Options for the Department of Defense*, RAND Report MR-1192-AF (Santa Monica, CA: RAND, 2000), 73-74. http://www.rand.org/ (accessed 22 April 2008).

[xxxviii] Ibid., 70.

[xxxix] Wilson, "Network Centric Operations," 6.

[xl] Mark Willoughby, "Hidden Malware in Offshore Products Raises Concerns," *Computerworld*, 15 September 2003. http://www.computerworld.com (accessed 22 April 2008).

[xli] U.S. DOD, *Military Power of China*, 28.

[xlii] Rebecca Grant, "The Dogs of Web War," *Air Force Magazine*, 1 January 2008, 23. http://www.proquest.com/ (accessed 22 April 2008).

[xliii] Demetri Sevastopulo, "Chinese Hacked into Pentagon," *Financial Times*, 3 September 2007. http://www.ft.com/ (accessed 22 April 2008).

[xliv] Glenn C. Buchanan, "Implications of Information Vulnerabilities for Military Operations" in *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND Report MR-1016-AF, ed. Zalmay Khalilzad et al. (Santa Monica, CA: RAND, 1999), 289. http://www.rand.org/ (accessed 22 April 2008).

[xlv]Ibid., 314.

[xlvi] Laurence Zuckerman, "Satellite Failure is Rare, and Therefore Unsettling," *New York Times*, 21 May 1998. http://www.nytimes.com/ (accessed 22 April 2008).

[xlvii] John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters* 32, no.4 (1 January 2003), 92. http://www.proquest.com/ (accessed April 22, 2008).

[xlviii] Wilson, "Network Centric Operations," 45.

[xlix] Dan Caterinicchia, "Marines Tunnel to SIPRNET," *Federal Computer Week*, 8 December 2002. http://www.fcw.com/ (accessed 22 April 2008).

Selected Bibliography

Bonds, Timothy, Michael Mattock, Thomas Hamilton, Carl Rhodes, Michael Scheiern, Phillip M. Feldman, David R. Frelinger, and Robert Uy. *Employing Commercial Satellite Communications: Wideband Investment Options for the Department of Defense*, RAND Report MR-1192-AF. Santa Monica, CA: RAND, 2000. http://www.rand.org/ (accessed 22 April 2008).

Brumbaugh, David A. "The Parallel Air Tasking Order: Reducing the Size of the Air Operations Center." Paper presented to the 2004 Command and Control Research and Technology Symposium, Chantilly, VA: Science Applications International Corp. (SAIC). http://www.dodccrp.org/ (accessed 22 April 2008).

Buchanan, Glenn C. "Implications of Information Vulnerabilities for Military Operations." In *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND Report MR-1016-AF, edited by Zalmay Khalilzad et al. Santa Monica, CA: RAND, 1999. http://www.rand.org/ (accessed 22 April 2008).

Caterinicchia, Dan. "Marines Tunnel to SIPRNET." *Federal Computer Week*, 8 December 2002. http://www.fcw.com/ (accessed 22 April 2008).

Chairman, U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms* (as Amended through 4 March 2008). Joint Publication (JP) 1-02. Washington, DC: CJCS, 2001. http://www.dtic.mil (accessed 22 April 2008).

Champagne, Lynne M. "Let's Put 'Joint' Back into JFACC." Research paper, Newport, RI: U.S. Naval War College, Department of Military Operations, 1994. http://stinet.dtic.mil/ (accessed 22 April 2008).

Cohen, Elliot A. "The Mystique of U.S. Air Power." *Foreign Affairs* 73, no. 1 (January 1, 1994): 109-124. http://www.proquest.com/ (accessed 22 April 2008).

Deputy Chief of Staff, Plans and Operations Headquarters, United States Air Force. *JFACC Primer*. Washington, DC: Headquarters Department of the Air Force, 10 January 1994. http://www.fas.org/ (accessed 22 April 2008).

Elegant, Simon and Mark Thompson. "Why China's Missile Test Is Troubling." *TIME*, 19 January 2007. http://www.time.com/ (accessed 12 April 2008).

Fyfe, John M. "The Evolution of Time Sensitive Targeting: Operation Iraqi Freedom Results and Lessons." Research paper no. 2005-02, Maxwell AFB, AL: Airpower Research Institute, 2005. http://stinet.dtic.mil/ (accessed 22 April 2008).

Gentry, John A. "Doomed to Fail: America's Blind Faith in Military Technology." *Parameters* 32, no. 4 (January 1, 2003): 88-103. http://www.proquest.com/ (accessed April 22, 2008).

Grant, Rebecca. "The Dogs of Web War." *Air Force Magazine*. 1 January 2008. http://www.proquest.com/ (accessed April 22, 2008).

Hebert, Adam J. "Toward Supremacy in Space." *Air Force Magazine*, January 1, 2005. http://www.afa.org/ (accessed 22 April 2008).

Hurley, Marcus. "JFACC – Taking the Next Step." *Joint Forces Quarterly* No. 7 (Spring 1995): 60-67. http://www.dtic.mil/ (accessed 22 April 2008).

Klausner, Kurt A. "Command and Control of Air and Space Forces Requires Significant Attention to Bandwidth." *Aerospace Power Journal*, 1 January 2002. http://www.proquest.com/ (accessed 22 April 2008).

Koprucu, Mustafa R. "The Limits of Decentralized Execution: The Effects of Technology on a Central Airpower Tenet." Research paper, Maxwell AFB, AL: School of Advanced Airpower Studies, 2001. http:stinet.dtic.mil/ (accessed 22 April 2008).

Parramore, Woody W. "Defining Decentralized Execution in Order to Recognize Centralized Execution." *Air & Space Power Journal*, 1 October 2004, 24-26. http://proquest.com/ (accessed 22 April, 2008).

Schaefer, John J. III. "Time for a New Master Tenet?" Research paper, Ft. Leavenworth, KS: School of Advanced Military Studies, 2006. http://stinet.dtic.mil/ (accessed 22 April 2008).

Sevastopulo, Demetri. "Chinese Hacked into Pentagon." *Financial Times*, 3 September 2007. http://www.ft.com/ (accessed 22 April 2008).

Shuman, Maxwell J. "Bringing a Grenade to a Knife Fight: Historical and Current Trends Challenge the Future Viability of the JFACC." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007. http://stinet.dtic.mil/ (accessed 22 April 2008).

Sink, J.T. "Rethinking the Air Operations Center: Air Force Command and Control in Conventional War." Research paper, Maxwell AFB, AL: School of Advanced Airpower Studies, 1994. http://stinet.dtic.mil/ (accessed 22 April 2008).

U.S. Air Force. *Air Force Basic Doctrine.* Air Force Doctrine Document (AFDD) 1. Washington, DC: Department of the Air Force, 17 November 2003. http://www.dtic.mil/ (accessed 22 April 2008).

U.S. Department of Defense. *Annual Report to Congress: Military Power of the People's Republic of China, 2008.* Washington, DC: Office of the Secretary of Defense, 2008. http:// hongkong.usconsulate.gov/ (accessed 22 April 2008).

War Department. *Command and Employment of Airpower*. War Department Field Manual (FM) 100-20. Washington, DC: GPO, 21 July 1943. http://www.au.af.mil/ (accessed 22 April 2008).

Willoughby, Mark. "Hidden Malware in Offshore Products Raises Concerns." *Computerworld*, 15 September, 2003. http://www.computerworld.com/ (accessed 22 April 2008).

Wilson, Clay. "Network Centric Operations: Background and Oversight Issues for Congress," CRS Report RL32411. Washington, DC: Congressional Research Service, 15 March 2007. http://www.fas.org/ (accessed 22 April 2008).

Winkler, Robert P. "The Evolution of the Joint ATO Cycle." Research paper, Norfolk, VA: Joint Forces Staff College, 2006. http://stinet.dtic.mil/ (accessed 22 April 2008).

Woodcock, William A. "The Joint Forces Air Command Problem: Is Network-Centric Warfare the Answer?" *Naval War College Review* 56, no. 1 (January 1, 2003): 124-138. http://www.proquest.com/ (accessed 22 April, 2008).

Zuckerman, Laurence. "Satellite Failure is Rare, and Therefore Unsettling." *New York Times,* 21 May 1998. http://www.nytimes.com/ (accessed 22 April 2008).